

## SEC 3.2 Security Services Functional Requirements

This section contains the requirements necessary to provide the Security Services for the DII COE. There is not a one-to-one mapping of the five broad areas of security services for the DII COE in section 3.1 to the subsections within this section. The mapping is shown in Table 1. Security Service Area Mapping to Subsection. Accountability requirements are presented in subsections for identification and authentication, and auditing; confidentiality requirements are presented in the discretionary access control, mandatory access control, labeling, markings, and object reuse subsections; and assurance requirements are presented in the subsections on System Architecture and Trusted Facility Management, and in Section SEC 3.16 and Section 4.

Security Service Area	Subsection
Accountability	Identification and Authentication (I&A), Trusted Path, Security Auditing
Access Control	Discretionary Access Control, Mandatory Access Control, Labels, Object Reuse
Confidentiality	Markings, Trusted Interfaces, Data Confidentiality
Integrity	Data Integrity, System Integrity, System Architecture, Trusted Facility Management
Non-repudiation	Non-repudiation
Availability	Availability

**Table 1. Security Service Area Mapping to Subsection**

### SEC 3.2.1 Identification and Authentication

3.2.1.1 The COE shall enforce individual accountability by providing the capability to uniquely identify each user to the system.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.1.1.1 The COE shall require users to uniquely identify themselves before beginning to perform any actions that the system is expected to mediate.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.1.1.2 The COE shall require login as an individual user before assuming a trusted profile (e.g., system administrator, security officer, root user, super user, etc.).

Traceability: DODIIS SAGD  
Priority 1

- 3.2.1.2 Each user shall be uniquely identifiable (e.g., user name or userID) within an administrative domain.  
Traceability: DOD 5200.28-STD  
GCCS Sec. Policy  
Priority 1
- 3.2.1.3 The COE shall provide the capability of associating the user's identity with all auditable actions taken by that individual.  
Traceability: DOD 5200.28-STD  
CSE-SS Seg. Spec.  
Priority 1
- 3.2.1.4 The COE shall use a mechanism (e.g., passwords) to authenticate each user's identity. If passwords are used as the mechanism, they shall meet the following requirements:  
Traceability: GCCS Sec. Policy  
CSE-SS Seg. Spec.  
Priority 1
- 3.2.1.4.1 The COE shall provide the capability for users, the security officer, or the system to generate passwords.  
Traceability: CSE-SS Seg. Spec.  
Priority 1
- 3.2.1.4.1.1 The COE shall provide a graphical user interface (GUI) for changing passwords.  
Traceability: CSE-SS Seg. Spec.  
Priority 1
- 3.2.1.4.1.2 The COE shall require a password be changed after the age of a password has exceeded a maximum defined by a trusted user.  
Traceability: Derived  
Priority 1
- 3.2.1.4.1.3 The COE shall notify the user prior to n days of password expiration where n is defined by a trusted user.  
Traceability: Derived  
Priority 1
- 3.2.1.4.1.4 The COE shall prohibit a password from being changed until the age of a password has exceeded a minimum defined by a trusted user.  
Traceability: Derived  
Priority 1
- 3.2.1.4.1.5 When changing the password, the COE shall prohibit the reuse of the current password and the password used previous to the current password.  
Traceability: Derived  
Priority 1
- 3.2.1.4.2 The COE shall ensure that passwords meet specific characteristics defined by a trusted user. These characteristics shall include the following:  
Traceability: Derived  
Priority 1
- 3.2.1.4.2.1 Minimum password length, which shall not be less than six characters  
Traceability: Derived  
Priority 1
- 3.2.1.4.2.2 Password character set (e.g., alphanumeric plus special ASCII characters)  
Traceability: Derived  
Priority 1

- 3.2.1.4.2.3 Password must include at least one numeric, case change, or special character (e.g., 0-9, &, %)
- Traceability: Derived  
Priority 1
- 3.2.1.4.2.4 Prohibit repeating characters (e.g., ee)
- Traceability: Derived  
Priority 1
- 3.2.1.4.2.5 Prohibit use of user name within password.
- Traceability: Derived  
Priority 1
- 3.2.1.5 The COE shall prevent unauthorized access to authentication data.
- Traceability: DOD 5200.28-STD  
Priority 1
- 3.2.1.5.1 The COE shall prevent unauthorized disclosure of passwords during transmission across a network.
- Traceability: DOD 5200.28-STD  
GCCS Sec. Policy  
Priority 2
- 3.2.1.5.2 The COE shall prevent unauthorized disclosure of passwords while stored.
- Traceability: DOD 5200.28-STD  
Priority 1
- 3.2.1.6 The COE shall provide the capability to restrict consecutive login failures.
- Traceability: CSE-SS Seg. Spec.  
Priority 1
- 3.2.1.6.1 If the number of consecutive login failures reaches a configurable threshold (0 through n), the userID shall be locked and the user shall be prohibited from further login attempts from within the administrative domain.
- Traceability: CSE-SS Seg. Spec.  
Priority 1
- 3.2.1.6.2 The default number of consecutive login failures shall be five.
- Traceability: CSE-SS Seg. Spec.  
Priority 1
- 3.2.1.6.3 If the number of multiple login failures is set to 0, the capability shall be disabled.
- Traceability: CSE-SS Seg. Spec.  
Priority 1
- 3.2.1.6.4 When a userID is locked, the COE shall send a notification to the security officer.
- Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.1.6.5 The COE shall provide the capability for a trusted user to restore locked userIDs.
- Traceability:  
Priority ???
- 3.2.1.7 The COE shall provide a non-forgeable, non-replayable distributed authentication mechanism that supports both unilateral (client-to-server) or mutual (client-to-server and server-to-client) authentication.
- Traceability: Arch Design Doc.  
Priority 2

## **SEC 3.2.2 Trusted Path**

3.2.2.1 The COE shall provide a trusted communication path between itself and the user for initial identification and authentication.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.2.2 The COE shall ensure that communication via the trusted communication path is initiated exclusively by a user.

Traceability: DOD 5200.28-STD  
Priority 3

## **SEC 3.2.3 Security Audit**

3.2.3.1 The COE shall provide the capability to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects.

Traceability: DOD 5200.28-STD  
GCCS Sec. Policy  
CSE-SS Seg. Spec.  
Priority 1

3.2.3.1.1 The COE shall protect audit data so that access to it is limited to those who are authorized to view audit data.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.3.1.2 The COE shall protect the audit processes and audit data from change or deletion by general users. At a minimum, the COE shall protect the following:

Traceability: DOD 5200.28 STD  
Priority 1

3.2.3.1.2.1 Audit mechanisms (e.g., executable files)

Traceability: Derived  
Priority 1

3.2.3.1.2.2 Configuration parameters (e.g., audit configuration files)

Traceability: Derived  
Priority 1

3.2.3.1.2.3 Capability to enable or disable Audit Processes

Traceability: Derived  
Priority 1

3.2.3.1.3 The COE shall provide a mechanism that generates a notification when the audit data has reached a configurable threshold of available storage capacity.

Traceability: GCCS Sec. Policy  
Derived  
Priority 1

3.2.3.1.3.1 The COE shall provide a capability for recovery in the event that available storage capacity has been exceeded. At a minimum, the following capabilities shall be provided:

- halt the system

Traceability: GCCS Sec. Policy  
Derived  
Priority 1

- overwrite previous audit data

	Traceability: GCCS Sec. Policy Derived Priority 1
<ul style="list-style-type: none"> <li>discontinue auditing</li> </ul>	Traceability: GCCS Sec. Policy Derived Priority 1
3.2.3.1.4 The COE shall provide a mechanism that generates a notification when the audit process(s) has failed.	Traceability: Derived Priority 2
3.2.3.1.4.1 The COE shall provide a capability for recovery in the event that the audit process(s) has failed. At a minimum, the following capabilities shall be provided:	
<ul style="list-style-type: none"> <li>halt the system</li> </ul>	Traceability: Derived Priority 2
<ul style="list-style-type: none"> <li>suspend processing until audit process(s) are restarted</li> </ul>	Traceability: Derived Priority 2
<ul style="list-style-type: none"> <li>discontinue auditing</li> </ul>	Traceability: Derived Priority 2
3.2.3.1.5 The COE shall provide a capability to archive audit data.	Traceability: GCCS Sec. Policy DOD 5200.28-STD Derived Priority 1
3.2.3.2 The COE shall provide the capability to enable and disable auditable events.	Traceability: DOD 5200.28-STD GCCS Sec. Policy Priority 1
3.2.3.3 The COE shall provide the capability to audit the following types of events:	Traceability: DOD 5200.28-STD Priority 1
3.2.3.3.1 Use of identification and authentication mechanisms	Traceability: DOD 5200.28-STD Priority 1
3.2.3.3.2 Introduction of objects into a user's address space (e.g., file open, program initiation)	Traceability: DOD 5200.28-STD Priority 1
3.2.3.3.3 Creation, modification, and deletion of objects	Traceability: DOD 5200.28-STD Priority 1
3.2.3.3.4 Actions taken by trusted users	Traceability: DOD 5200.28-STD Priority 1

3.2.3.3.5	Production of printed output	Traceability: DOD 5200.28-STD Priority 1
3.2.3.3.6	Override of human-readable output markings	Traceability: CSE-SS Reqs. Priority 1
3.2.3.3.7	Change in access control permissions	Traceability: DOD 5200.28-STD Priority 1
3.2.3.3.8	Export to external media	Traceability: DODIIS SAGD Priority 1
3.2.3.3.9	System startup	Traceability: DODIIS SAGD Priority 1
3.2.3.3.10	System shutdown.	Traceability: DODIIS SAGD Priority 1
3.2.3.4	The COE shall provide the capability for a trusted user to define security relevant events.	Traceability: Derived Priority 2
3.2.3.5	For each recorded event, at a minimum the COE audit record shall identify:	Traceability: DOD 5200.28-STD Priority 1
3.2.3.5.1	System date and time (to the nearest second) of the event	Traceability: DOD 5200.28-STD Priority 1
3.2.3.5.2	UserID	Traceability: DOD 5200.28-STD Priority 1
3.2.2.5.3	Type of event	Traceability: DOD 5200.28-STD Priority 1
3.2.3.5.4	Success or failure of the event	Traceability: DOD 5200.28-STD Priority 1
3.2.3.6	For identification and authentication events, the COE audit record shall identify the origin of the request (e.g., terminal ID, host IP address)	Traceability: DOD 5200.28-STD Priority 1
3.2.3.7	For events that introduce an object into a user's address space, and for object deletion events, the COE audit record shall identify the name of the object, and in MLS systems, the object's security level (e.g., sensitivity level and handling caveats).	Traceability: DOD 5200.28-STD Priority 1

3.2.3.8 The COE shall provide the capability to selectively audit the actions of any one or more users based on individual identity.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.3.9 The COE shall provide the capability to correlate all system administrative and audit logs (e.g., database management system logs, operating system audit logs, and other system logs) within an administrative domain.

Traceability: DOD 5200.28-STD  
Derived  
Priority 2

3.2.3.10 The COE shall provide the capability to receive application level audit data (e.g., Unix syslog, Windows NT event log).

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.3.11 The COE shall provide the capability to generate reports of audit data that has been collected.

Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

3.2.3.11.1 The COE shall provide the capability to generate reports based on fields of event records or Boolean combinations of those fields.

Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

3.2.3.11.2 The COE shall provide the capability to generate reports based on ranges of system date and time that audit records were collected.

Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

## **SEC 3.2.4 Availability**

3.2.4.1 The COE shall be capable of detecting the failure of a security service or resource.

Traceability: GCCS Sec. Policy  
Derived  
Priority 2

3.2.4.1.1 Failure of a COE security service or resource shall generate an alert.

Traceability: GCCS Sec. Policy  
Derived  
Priority 2

3.2.4.2 Upon recovery of a system resource, the COE shall verify that it returns in a secure state.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.4.3 The COE shall provide the capability to selectively deny service to users.

Traceability: GCCS Sec. Policy  
Derived  
Priority 1

3.2.4.4 The COE shall provide the capability to perform system and database backups.  
Traceability: DOD 5200.28-STD  
CSE-SS Seg. Spec.  
GCCS Sec. Policy  
Priority 1

3.2.4.5 The COE shall provide the capability to recover from failures using system and database backups.  
Traceability: DOD 5200.28-STD  
CSE-SS Seg. Spec.  
GCCS Sec. Policy  
Priority 1

### **SEC 3.2.5 Discretionary Access Control (DAC)**

3.2.5.1 The COE shall provide the capability to define access between named users and named objects (e.g., files, database elements, and programs).

Traceability: DOD 5200.28-STD  
Priority 1

3.2.5.2 The COE shall provide the capability to control access between named users and named objects (e.g., files, database elements, and programs).

Traceability: DOD 5200.28-STD  
Priority 1

3.2.5.3 The COE shall restrict access to objects based on the user's identity and on access rights (e.g., read, write, execute).

Traceability: DOD 5200.28-STD  
Priority 1

3.2.5.4 The COE shall provide the capability for users to specify and control sharing of objects by named users or defined sets of users (e.g., UNIX groups, access control lists), or by both.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.5.5 The COE shall provide controls to limit the propagation of access rights.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.5.6 The COE shall, either by explicit user action or by default, protect objects from unauthorized access.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.5.7 The COE shall provide the capability to assign access rights to authorized users.

Traceability: GCCS Sec. Policy  
Priority 1

3.2.5.8 The COE shall permit a user to grant or revoke access to an object only if the user has control permission (e.g., file owner) to that object.

Traceability: DOD 5200.28-STD  
GCCS Sec. Policy  
Derived  
Priority 1

3.2.5.9 The COE shall provide a means to associate applications with a work environment (i.e., profiles) and allow users to specify the work environment (i.e., profile selection) during a session.

Traceability: CSE-SS Seg. Spec.  
DODIIS SAGD  
Priority 1

3.2.5.9.1 The COE shall permit a user to hold membership in multiple groups of users and have the access rights of those groups simultaneously.

Traceability: Derived  
Priority 1

3.2.5.10 The COE shall provide the capability to maintain logical separation among users (e.g., through separate address space, processes, etc.).

Traceability: DOD 5200.28-STD  
Priority 1

3.2.5.11 The COE shall be capable of restricting access to input/output (I/O) devices (e.g., floppy disks and tape drives).

Traceability: DODIIS SAGD  
Priority 1

3.2.5.11.1 The COE shall provide a capability to specify which users may access which I/O devices.

Traceability: DODIIS SAGD  
Derived  
Priority 1

3.2.5.12 The COE shall provide a deadman capability that locks the user's terminal if user input devices have been idle for longer than a configurable time period of zero to n minutes.

Traceability: CSE-SS Seg. Spec.  
DODIIS SAGD  
Priority 1

3.2.5.12.1 The configurable time period shall default to 5 minutes.

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.5.12.2 If the configurable time period is set to zero, the deadman capability shall be disabled.

Traceability: Derived  
Priority 1

3.2.5.12.3 Any user input device may be used to initiate actions to restore a locked terminal.

Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

3.2.5.12.4 The specific input value (whether from keyboard, mouse, or other input device) used to activate restoration of the locked terminal shall be ignored except to initiate actions to unlock the terminal.

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.5.12.5 The COE shall require that users re-authenticate themselves to unlock a locked terminal.

Traceability: Derived  
Priority 1

3.2.5.12.6 The deadman capability shall be available for users to manually invoke.

Traceability: Derived  
Priority 1

## **SEC 3.2.6 Mandatory Access Control (MAC)1**

3.2.6.1 The COE shall enforce a mandatory access control (MAC) policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the COE Security Services.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.6.1.1 Subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical levels and categories, and the labels shall be used as the basis for mandatory access control decisions.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.6.1.2 The COE shall support three or more hierarchical levels

Traceability: Derived  
Priority 3

3.2.6.1.3 The COE shall support a minimum of 128 categories.

Traceability: Derived  
Priority 3

3.2.6.2 The COE shall mediate all accesses between subjects and objects providing:

Traceability: DOD 5200.28-STD  
Priority 3

3.2.6.2.1 A subject can read an object only if the classification in the subject's security level is greater than or equal to the classification in the object's security level and the categories in the subject's security level include all the categories in the object's security level.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.6.2.2 A subject can write an object only if the classification in the subject's security level is less than or equal to the classification in the object's security level and all the categories in the subject's security level are included in the categories of the object's security level.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.6.3 The COE shall ensure that the security level and authorization of subjects created to act on behalf of the individual user are dominated by the clearance and authorization of that user prior to data access.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.6.4 The COE shall provide the capability for authorized users to change the sensitivity label (e.g., upgrade or downgrade) of an object.

Traceability: Derived  
Priority 3

3.2.6.4.1 The COE shall provide the capability to audit any change of sensitivity label.

Traceability: DOD 5200.28-STD  
Priority 3

---

IMAC requirements are the B2 requirements from DOD 5200.28-STD. Not all COE components will need to implement MAC. MAC will be implemented incrementally as operational considerations require MLS mode and technology permits.

## **SEC 3.2.7      Sensitivity Labels<sup>2</sup>**

- 3.2.7.1 The COE shall maintain sensitivity labels that are associated with each system resource (e.g., subject, storage object, ROM) directly or indirectly accessible by subjects external to the COE.

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.1.1 Sensitivity labels shall be used as the basis for mandatory access control decisions.

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.1.2 To import non-labeled data, the COE shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the COE.

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.2 The COE shall ensure that sensitivity labels accurately represent security levels of the specific subjects or objects with which they are associated.

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.2.1 When exported by the COE, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported (e.g., internal labels for an object would need to accurately map to Common Internet Protocol Security Option labels used during network transmissions).

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.3 The COE shall designate each communication channel and I/O device as either single-level or multilevel.

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.3.1 Any change in the designation of single-level or multilevel shall be done manually by an authorized user.

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.3.2 The COE shall provide the capability to audit any change in single-level or multilevel designation.

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.3.3 When the COE exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form).

Traceability: DOD 5200.28-STD  
Priority 3

- 3.2.7.3.4 When the COE exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

Traceability: DOD 5200.28-STD  
Priority 3

---

<sup>2</sup>Sensitivity labels are required for MLS mode.

3.2.7.3.5 The COE shall include a mechanism by which the COE and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.7.3.6 The COE shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.7.3.7 The COE shall provide the capability for a terminal user to query the COE for a display of the subject's complete sensitivity label.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.7.3.8 The COE shall assign minimum and maximum sensitivity levels to all attached physical devices.

Traceability: DOD 5200.28-STD  
Priority 3

## **SEC 3.2.8 Markings**

3.2.8.1 The COE shall display a security warning prior to the login process that indicates the highest classification of information processed on the system.

Traceability: DODIIS SAGD  
Priority 1

3.2.8.2 The COE shall display a security warning during the login process that indicates misuse of the system is subject to applicable penalties.

Traceability: DODIIS SAGD  
Priority 1

3.2.8.2.1 This security warning shall state that the user accepts responsibility for his or her actions prior to being permitted to access information.

Traceability: Derived  
Priority 1

3.2.8.3 The COE shall provide the capability to surround each print job with banner pages reflecting the system high level of the system.

Traceability: DOD Dir. 5200.28  
CSE-SS Seg. Spec.  
Priority 1

3.2.8.3.1 When operating in the multilevel mode, the COE shall mark the beginning and end of all printed output with human-readable sensitivity labels that properly represent the sensitivity of the output.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.8.4 The COE shall provide the capability to label the top and bottom of each internal page of printed output with a sensitivity label representing the sensitivity of the output.

Traceability: CSE-SS Seg. Spec  
Priority 1

3.2.8.4.1 The internal page markings shall default to the system high label of the system.

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.8.4.2 When operating in the multilevel mode, markings on internal pages shall properly represent the sensitivity of the output.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.8.5 The COE shall provide the user with print options to override the printing of the banner pages and internal page markings.

Traceability: DOD 5200.28-STD  
Priority 3

3.2.8.5.1 The COE shall provide the capability to audit any override of the printing of banner pages and internal page markings.

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.8.6 The COE shall provide the following forms of markings for labeling printed output:

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.8.6.1 Highest classification of information processed on the system

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.8.6.2 Markings that represent the actual security level (classification and compartments) of the information being printed

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.8.6.3 Applicable markings (codewords, dissemination and control markings and handling caveats).

Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.8.7 The COE shall provide a GUI-based interface from which the user selects the destination printer, number of copies, sensitivity label from the set of authorized markings.

Traceability: CSE-SS Seg. Spec.  
Priority 1

## **SEC 3.2.9 Trusted Interfaces**

3.2.9.1 The COE shall provide a capability to review and release information to systems of disparate security levels.

Traceability: GCCS Sec. Policy  
Priority 2

3.2.9.2 The COE shall provide the capability to audit the release of information to systems of disparate security levels.

Traceability: GCCS Sec. Policy  
Priority 2

### **SEC 3.2.10 Object Reuse**

3.2.10.1 The COE shall ensure that no information, including encrypted representations of information, produced by a prior subject's actions is made available to any subject that obtains access to an object that has been released back to the COE.

Traceability: DOD 5200.28-STD  
GCCS Sec. Policy  
Priority 1

3.2.10.2 The COE shall ensure that all authorizations to information contained within a storage object have been revoked prior to initial assignment, allocation, or reallocation to a subject from the COE's pool of unused storage objects.

Traceability: DOD 5200.28-STD  
GCCS Sec. Policy  
Priority 1

### **SEC 3.2.11 Data Confidentiality**

3.2.11.1 The COE shall provide an interface to cryptographic application programming interfaces for use by applications to selectively encrypt and decrypt data and files.

Traceability: GCCS Sec. Policy  
Priority 2

### **SEC 3.2.12 Data Integrity**

3.2.12.1 The COE shall provide the capability to detect unauthorized modification or destruction of data during storage (e.g., using digital signatures and hash codes on files).

Traceability: DOD 5200.28-STD  
GCCS Sec. Policy  
Priority 1

3.2.12.1.1 The COE shall provide the capability to audit unauthorized modification or destruction of data during storage.

Traceability: Derived  
Priority 2

3.2.12.2 The COE shall provide the capability to detect modification or destruction of data that occur while in transit over communications channels (e.g., using cryptographic checksums or digital signatures).

Traceability: GCCS Sec. Policy  
Derived  
Priority 2

### **SEC 3.2.13 System Integrity**

3.2.13.1 The COE shall provide the capability to validate the correct operation of the hardware, software and firmware elements of the COE Security Services.

Traceability: DOD 5200.28-STD  
GCCS Sec. Policy  
Priority 1

3.2.13.2 The COE shall provide the capability to automatically validate the correct operation of the hardware and firmware elements of the COE Security Services during recovery from failure.

Traceability: DOD 5200.28-STD  
Priority 1

3.2.13.3 The COE shall be configured such that a password must be entered to boot to a single-user state.  
Traceability: DODIIS SAGD  
Priority 1

#### **SEC 3.2.14 Non-repudiation**

3.2.14.1 The COE shall provide the capability for the recipient of an information transaction to determine proof of the origin and originator of the data (e.g., using digital signatures).  
Traceability: TAFIM Vol. 6  
Priority 3

3.2.14.2 The COE shall provide the capability for the sender of an information transaction to determine proof of delivery (e.g., using digital signatures).  
Traceability: TAFIM Vol. 6  
Priority 3

#### **SEC 3.2.15 System Architecture**

3.2.15.1 The COE Security Services shall maintain a domain for their own execution that protects them from external interference or tampering (e.g., by modification of their code or data structures).  
Traceability: DOD 5200.28-STD  
Priority 1

3.2.15.2 The COE shall isolate resources to be protected so that they are subject to the access control and auditing requirements.  
Traceability: DOD 5200.28-STD  
Priority ???

3.2.15.3 The COE shall implement the principle of least principle such that each subject is granted the most restrictive set of privileges needed for the performance of authorized tasks.  
Traceability: DOD 5200.28-STD  
DDS-2600-5502-87  
Priority 1

#### **SEC 3.2.16 Trusted Facility Management**

3.2.16.1 The COE shall support trusted facility management via segregation of authorized roles.  
Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.16.1.1 At a minimum the COE shall provide security officer, systems administrator, and user roles.  
Traceability: CSE-SS Seg. Spec.  
Priority 1

3.2.16.1.2 The COE shall provide the capability to create trusted roles.  
Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

3.2.16.1.3 The COE shall provide the capability to assign security relevant functions to a trusted role.  
Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

- 3.2.16.1.4 The COE shall provide the capability to modify trusted roles.  
Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.1.4.1 The COE shall provide the capability to add security relevant functions to a trusted role.  
Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.1.4.2 The COE shall provide the capability to delete security relevant functions to a trusted role.  
Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.1.5 The COE shall provide the capability to delete trusted roles.  
Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.1.6 The COE shall prohibit security relevant functions from being assigned to non-trusted roles.  
Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.2 The COE shall provide the capability to manage accounts for authorized users.  
Traceability: DOD 5200.28 STD  
CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.2.1 The COE shall provide the capability to create accounts for authorized users.  
Traceability: DOD 5200.28-STD  
CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.2.2 The COE shall provide the capability to modify accounts for authorized users.  
Traceability: DOD 5200.28-STD  
CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.2.3 The COE shall provide the capability to delete accounts for authorized users.  
Traceability: DOD 5200.28-STD  
CSE-SS Seg. Spec.  
Derived  
Priority 1
- 3.2.16.3 The COE shall provide the capability to manage profiles for groups of users with common access rights.  
Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

3.2.16.3.1 The COE shall provide the capability to create profiles or groups of users with common access rights.

Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

3.2.16.3.2 The COE shall provide the capability to modify the access rights of profiles or groups of users.

Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

3.2.16.3.3 The COE shall provide the capability to delete profiles or groups of users.

Traceability: CSE-SS Seg. Spec.  
Derived  
Priority 1

3.2.16.4 The COE shall provide the capability to purge data from fixed and removable storage media or assignable storage devices.

Traceability: GCCS Sec. Policy  
Derived  
Priority 1

3.2.16.5 The COE shall provide a standard set of security support tools to determine the security posture of COE systems.

Traceability: DODIIS SAGD  
Derived  
Priority 2

3.2.16.5.1 The COE shall provide the capability to validate that passwords have met the requirements for password characteristics specified in paragraph 3.2.1.4.2.

Traceability: DODIIS SAGD  
Derived  
Priority 2

3.2.16.5.2 The COE shall provide the capability to determine if changes have been made to designated systems and applications files, (e.g., password or rc.\* files).

Traceability: DODIIS SAGD  
Derived  
Priority 2

3.2.16.5.3 The COE shall provide the capability for a trusted user to monitor and analyze the configuration of a host.

Traceability: DODIIS SAGD  
Derived  
Priority 1

3.2.16.6 The COE shall provide the capability to manage sensitivity labels and handling caveats used in marking printed output.

Traceability: Derived  
Priority 1

3.2.16.6.1 The COE shall provide the capability to enable or disable marking printed output with sensitivity labels and handling caveats.

Traceability: Derived  
Priority 2

3.2.16.6.2 The COE shall provide a GUI-based capability for creating a set of authorized sensitivity labels and handling caveat values for use in marking printed output.

Traceability: Derived  
Priority 2

3.2.16.6.3 The COE shall provide a GUI-based capability for modifying the set of authorized sensitivity labels and handling caveat values that are used in marking printed output.

Traceability: Derived  
Priority 2

3.2.16.6.4 The COE shall provide a GUI-based capability for deleting of the set of authorized sensitivity label and handling caveat values that are used in marking printed output.

Traceability: Derived  
Priority 2